SHORT PROJECT

PHASE TWO

HAFIZ NAVEED UDDIN, KAIRIZ CYBER TECHOLOGIES

Phase 2: Penetration Testing Report

1. **External Penetration Test**
   - **Objective:** Conducted an external penetration test to identify vulnerabilities exploitable by attackers from outside the network.
   - **Tools Used:** Metasploit, Burp Suite, OWASP ZAP
   - **Findings:**
     - Identified open ports susceptible to remote exploitation.
     - Discovered potential weaknesses in firewall configurations.
     - Documented vulnerabilities with proof-of-concept exploits.
2. **Internal Penetration Test**
   - **Objective:** Conducted an internal penetration test to identify vulnerabilities exploitable by insiders or through lateral movement.
   - **Focus Areas:** Privilege escalation, lateral movement, sensitive data access.
   - **Findings:**
     - Successfully escalated privileges on several systems.
     - Identified weaknesses in internal network segmentation.
     - Documented pathways for lateral movement and access to sensitive data.
3. **Web Application Security Assessment**
   - **Objective:** Performed a thorough security assessment of web applications present in the environment.
   - **Focus:** Common vulnerabilities such as SQL injection, XSS, insecure authentication mechanisms.
   - **Findings:**
     - Discovered SQL injection vulnerabilities in web application forms.
     - Identified XSS vulnerabilities allowing script injection.
     - Documented insecure authentication mechanisms posing risks to user data.
4. **Summary of Findings**
   - **Overall Assessment:** The network and web applications exhibit significant vulnerabilities that could be exploited by malicious actors.
   - **Key Issues Identified:**
     - Open ports susceptible to remote exploitation.
     - Firewall configurations need strengthening to prevent unauthorized access.
     - Privilege escalation and lateral movement pathways exist within the internal network.
     - Critical vulnerabilities in web applications pose risks to data integrity and user confidentiality.
5. **Recommendations**
   - **Immediate Actions:**
     - Patch and update systems to address identified vulnerabilities.
     - Enhance firewall configurations to restrict unnecessary open ports.
     - Implement strong authentication mechanisms for web applications.
   - **Long-term Strategies:**
     - Regular penetration testing and security assessments to proactively identify new vulnerabilities.

        - Continuous monitoring of network and application logs for suspicious activities.
        - Employee training on cybersecurity best practices and social engineering awareness.

6. **Conclusion**
    - The penetration testing activities have provided valuable insights into the current security posture of the network and web applications. Immediate actions are recommended to mitigate identified risks and enhance overall security resilience.